PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of

Masanori SATAKE et al.

Application No.: 10/653,191

Filed: September 3, 2003 Docket No.: 116971

For: APPARATUS AND METHOD FOR SECURELY REALIZING COOPERATIVE PROCESSING

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2003-082612 Filed March 25, 2003

In support of this claim, a certified copy of said original foreign application:

__x__ is filed herewith.

_____ was filed on _____ in Parent Application No. _____ filed _____.

_____ will be filed at a later date.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Joel S. Armstrong
Registration No. 36,430

THOMAS J. PARDINI
Reg. No. 30,411

JAO:JSA/emt

Date: October 14, 2003

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年　３月２５日

出 願 番 号
Application Number: 特願２００３－０８２６１２

[ST. 10/C]: ［ＪＰ２００３－０８２６１２］

出 願 人
Applicant(s): 富士ゼロックス株式会社

２００３年　９月１０日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０７４２２８

【書類名】　特許願
【整理番号】　FE03-00266
【提出日】　平成15年 3月25日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/00
【発明者】
　【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社内
　【氏名】　佐竹　雅紀
【発明者】
　【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社内
　【氏名】　益井　隆徳
【発明者】
　【住所又は居所】　神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社内
　【氏名】　横濱　竜彦
【特許出願人】
　【識別番号】　000005496
　【氏名又は名称】　富士ゼロックス株式会社
【代理人】
　【識別番号】　100075258
　【弁理士】
　【氏名又は名称】　吉田　研二
　【電話番号】　0422-21-2340

【選任した代理人】

【識別番号】　100096976

【弁理士】

【氏名又は名称】　石田　純

【電話番号】　0422-21-2340

【手数料の表示】

【予納台帳番号】　001753

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置、ジョブ処理装置、指示データ作成装置及び署名プロキシ装置

【特許請求の範囲】

【請求項１】　ジョブ処理を指示する処理記述が記述された指示データ、またはジョブ処理の対象となる被処理データをジョブ処理装置に送信し、ジョブ処理を実行させる情報処理装置であって、

第１の認証機関により認証された第１の署名鍵と、第２の認証機関により認証された第２の署名鍵のいずれで指示データまたは被処理データに署名するかを切り換える切換部と、

前記切換部により切り換えられた署名鍵で、前記指示データまたは前記被処理データに署名を施す署名部と、

前記署名部により署名された指示データまたは被処理データを前記ジョブ処理装置に向けて送信する送信部と、

を備えることを特徴とする情報処理装置。

【請求項２】　請求項１に記載の情報処理装置において、

第１の署名鍵を認証するのは不特定多数の利用者を認証する認証機関であり、第２の署名鍵を認証するのは所定の利用者を認証する認証機関であることを特徴とする情報処理装置。

【請求項３】　請求項１に記載の情報処理装置において、

前記切換部は、前記ジョブ処理装置の属性に応じて切り換えることを特徴とする情報処理装置。

【請求項４】　請求項３に記載の情報処理装置において、

ジョブ処理装置の属性とは、所定のネットワーク内にジョブ処理装置が位置しているか否かであることを特徴とする情報処理装置。

【請求項５】　ジョブ処理を指示する処理記述が記述された指示データ、またはジョブ処理の対象となる被処理データをジョブ処理装置に送信し、ジョブ処理を実行させる情報処理方法であって、

第１の認証機関により認証された第１の署名鍵と、第２の認証機関により認証

された第２の署名鍵のいずれで指示データまたは被処理データに署名するかを切り換え、

この切り換えにより選択された署名鍵で、前記指示データまたは前記被処理データに電子署名を施し、

前記署名部により電子署名が施された指示データまたは被処理データを前記ジョブ処理装置に向けて送信する、

情報処理方法。

【請求項６】　ジョブ処理を指示する処理記述が記述された指示データ、またはジョブ処理の対象となる被処理データをジョブ処理装置に送信し、ジョブ処理を実行させるコンピュータのプログラムであって、

コンピュータに、

第１の認証機関により認証された第１の署名鍵と、第２の認証機関により認証された第２の署名鍵のいずれで指示データまたは被処理データに署名するかを切り換える手順と、

この切り換えにより選択された署名鍵で、前記指示データまたは前記被処理データに電子署名を施す手順と、

前記署名部により電子署名が施された指示データまたは被処理データを前記ジョブ処理装置に向けて送信する手順と、

を実行させるためのプログラム。

【請求項７】　自装置が属するネットワークの内部用と外部用にそれぞれ別の署名鍵を有する鍵記憶部と、

各ジョブ処理装置に対する処理指示と各ジョブ処理装置の次のジョブ処理装置とを示したフロー指示データを受信する受信部と、

前記受信部で受信したフロー指示データに付与された電子署名を検証する署名検証部と、

前記署名検証部による検証が成功した場合に、前記フロー指示データ内から自装置が実行すべき処理指示を識別し、その処理指示に従って処理を実行する処理部と、

前記処理部により処理を実行した場合に、前記受信したフロー指示データを基

に、自装置の次のジョブ処理装置に送信する出力フロー指示データを作成する指示データ作成部と、

前記次のジョブ処理装置が前記ネットワーク内の装置か否かを判定する判定部と、

前記次のジョブ処理装置が前記ネットワーク内の装置である場合には前記内部用の署名鍵を用い、そうでない場合は前記外部用の署名鍵を用いて、前記出力フロー指示データに電子署名を付与する署名処理部と、

前記署名処理部で電子署名が付与された出力フロー指示データを前記次のジョブ処理装置に送信する送信部と、

を備えるジョブ処理装置。

【請求項８】　請求項７記載の装置であって、

前記判定部は、前記フロー指示データ中に示された自装置の次のジョブ処理装置のインターネット上での位置情報に基づき、当該次のジョブ処理装置が前記ネットワーク内か否かを判定することを特徴とするジョブ処理装置。

【請求項９】　フロー指示データに従って他のジョブ処理装置と連携してサービスを実行するジョブ処理装置におけるフロー指示データの処理方法であって、

各ジョブ処理装置に対する処理指示と各ジョブ処理装置の次のジョブ処理装置とを示したフロー指示データを受信し、

前記受信部で受信したフロー指示データに付与された電子署名を検証し、

前記署名検証部による検証が成功した場合に、前記フロー指示データ内から自装置が実行すべき処理指示を識別し、

識別した処理指示に従って処理を実行し、

前記処理指示を実行した場合に、前記受信したフロー指示データを基に、自装置の次のジョブ処理装置に送信する出力フロー指示データを作成し、

前記次のジョブ処理装置が前記ネットワーク内の装置か否かを判定し、

前記次のジョブ処理装置が前記ネットワーク内の装置である場合には、自装置が属するネットワークの内部用の署名鍵を用い、そうでない場合は前記ネットワークの外部用の署名鍵を用いて、前記出力フロー指示データに電子署名を付与し

、

電子署名が付与された前記出力フロー指示データを前記次のジョブ処理装置に送信する、

方法。

【請求項１０】　コンピュータシステムを、

自装置が属するネットワークの内部用と外部用にそれぞれ別の署名鍵を有する鍵記憶部と、

各ジョブ処理装置に対する処理指示と各ジョブ処理装置の次のジョブ処理装置とを示したフロー指示データを受信する受信部と、

前記受信部で受信したフロー指示データに付与された電子署名を検証する署名検証部と、

前記署名検証部による検証が成功した場合に、前記フロー指示データ内から自装置が実行すべき処理指示を識別し、その処理指示に従って処理を実行する処理部と、

前記処理部により処理を実行した場合に、前記受信したフロー指示データを基に、自装置の次のジョブ処理装置に送信する出力フロー指示データを作成する指示データ作成部と、

前記次のジョブ処理装置が前記ネットワーク内の装置か否かを判定する判定部と、

前記次のジョブ処理装置が前記ネットワーク内の装置である場合には前記内部用の署名鍵を用い、そうでない場合は前記外部用の署名鍵を用いて、前記出力フロー指示データに電子署名を付与する署名処理部と、

前記署名処理部で電子署名が付与された出力フロー指示データを前記次のジョブ処理装置に送信する送信部と、

して機能させるためのプログラム。

【請求項１１】　各ジョブ処理装置に対する処理指示と各ジョブ処理装置の次のジョブ処理装置とを示したフロー指示データをそれら各ジョブ処理装置間で順に受け渡しながら、それら各ジョブ処理装置がそれぞれ自装置に対する処理指示を順に実行することでサービスを実現するシステムのために、前記フロー指示

データを作成する指示データ作成装置であって、

当該指示データ作成装置が属するネットワークの内部用の署名鍵と外部用の署名鍵とを有する鍵記憶部と、

前記サービスのためのジョブ処理装置群の中に、前記ネットワークの外部にあるジョブ処理装置が含まれているか否かを判定する判定部と、

前記サービスのためのジョブ処理装置群の中に前記ネットワークの外部にある装置が含まれていると前記判定部で判定された場合は前記外部用の署名鍵を用い、そうでない場合は前記内部用の署名鍵を用いて前記フロー指示データに電子署名を付与する署名処理部と、

前記署名処理部で電子署名が付与されたフロー指示データを前記サービスにおけるジョブ処理装置群の中の最初のジョブ処理装置に送信する送信部と、

を備える指示データ作成装置。

【請求項１２】　請求項１１記載の装置であって、

前記判定部は、前記フロー指示データ中に示された自装置の次のジョブ処理装置のインターネット上での位置情報に基づき、当該次のジョブ処理装置が前記ネットワーク内か否かを判定することを特徴とするジョブ処理装置。

【請求項１３】　各ジョブ処理装置に対する処理指示と各ジョブ処理装置の次のジョブ処理装置とを示したフロー指示データをそれら各ジョブ処理装置間で順に受け渡しながら、それら各ジョブ処理装置がそれぞれ自装置に対する処理指示を順に実行することでサービスを実現するシステムのために、コンピュータシステムにより前記フロー指示データを作成する方法であって、

前記サービスのためのジョブ処理装置群の中に、前記ネットワークの外部にあるジョブ処理装置が含まれているか否かを判定し、

前記サービスのためのジョブ処理装置群の中に前記ネットワークの外部にある装置が含まれていると前記判定部で判定された場合は、当該指示データ作成装置が属するネットワークの外部用の署名鍵を用い、そうでない場合は前記ネットワークの内部用の署名鍵を用いて前記フロー指示データに電子署名を付与し、

電子署名が付与されたフロー指示データを前記サービスにおけるジョブ処理装置群の中の最初のジョブ処理装置に送信する、

方法。

【請求項１４】　各ジョブ処理装置に対する処理指示と各ジョブ処理装置の次のジョブ処理装置とを示したフロー指示データをそれら各ジョブ処理装置間で順に受け渡しながら、それら各ジョブ処理装置がそれぞれ自装置に対する処理指示を順に実行することでサービスを実現するシステムのために、前記フロー指示データを作成するコンピュータのプログラムであって、

コンピュータを、

当該指示データ作成装置が属するネットワークの内部用の署名鍵と外部用の署名鍵とを有する鍵記憶部と、

前記サービスのためのジョブ処理装置群の中に、前記ネットワークの外部にあるジョブ処理装置が含まれているか否かを判定する判定部と、

前記サービスのためのジョブ処理装置群の中に前記ネットワークの外部にある装置が含まれていると前記判定部で判定された場合は前記外部用の署名鍵を用い、そうでない場合は前記内部用の署名鍵を用いて前記フロー指示データに電子署名を付与する署名処理部と、

前記署名処理部で電子署名が付与されたフロー指示データを前記サービスにおけるジョブ処理装置群の中の最初のジョブ処理装置に送信する送信部と、

して機能させるためのプログラム。

【請求項１５】　内部ネットワークと外部ネットワークとの間に介在し、該内部ネットワーク上の装置と前記外部ネットワーク上の装置との間で文書のやりとりを媒介するプロキシ装置であって、

前記内部ネットワーク上の装置から前記外部ネットワーク上の装置に送信される文書に付された電子署名を検証する第１署名検証部と、

前記第１署名検証部による検証によりその文書に付された電子署名が内部ネットワーク用の署名鍵を用いたものであることが分かった場合は、前記文書からその電子署名を削除し、前記文書に対して当該署名プロキシ装置の外部ネットワーク用の署名鍵を用いて電子署名を付与し直して、前記外部ネットワーク上の前記装置へと送信する第１署名変換部と、

を備える署名プロキシ装置。

【請求項１６】　請求項１５記載のプロキシ装置であって、

前記外部ネットワーク上の装置から前記内部ネットワーク上の装置に送信される文書に付された電子署名を検証する第２署名検証部と、

前記第２署名検証部による検証が成功した場合、その文書からその電子署名を削除し、その文書に対して当該署名プロキシ装置の内部ネットワーク用の署名鍵を用いて電子署名を付与し直して、前記内部ネットワーク上の前記装置へと送信する第２署名変換部と、

を更に備える署名プロキシ装置。

【請求項１７】　内部ネットワークと外部ネットワークとの間に介在するプロキシ装置において、該内部ネットワーク上の装置と前記外部ネットワーク上の装置との間で文書のやりとりを媒介する方法であって、

前記内部ネットワーク上の装置から前記外部ネットワーク上の装置に送信される文書に付された電子署名を検証し、

この検証によりその文書に付された電子署名が内部ネットワーク用の署名鍵を用いたものであることが分かった場合、前記文書からその電子署名を削除し、

その電子署名を削除した前記文書に対して当該署名プロキシ装置の外部ネットワーク用の署名鍵を用いて電子署名を付与し直し、

前記外部ネットワーク用の署名鍵を用いて電子署名を付与し直した前記文書を前記外部ネットワーク上の前記装置へと送信する、

文書通信媒介方法。

【請求項１８】　内部ネットワークと外部ネットワークとの間に介在し、該内部ネットワーク上の装置と前記外部ネットワーク上の装置との間で文書のやりとりを媒介するコンピュータのプログラムであって、

コンピュータを、

前記内部ネットワーク上の装置から前記外部ネットワーク上の装置に送信される文書に付された電子署名を検証する第１署名検証部と、

前記第１署名検証部による検証によりその文書に付された電子署名が内部ネットワーク用の署名鍵を用いたものであることが分かった場合は、前記文書からその電子署名を削除し、前記文書に対して当該署名プロキシ装置の外部ネットワー

ク用の署名鍵を用いて電子署名を付与し直して、前記外部ネットワーク上の前記装置へと送信する第１署名変換部と、

と機能させるためのプログラム。

【請求項１９】　内部ネットワークと外部ネットワークとの間に介在し、該内部ネットワーク上の装置と前記外部ネットワーク上の装置との間で文書のやりとりを媒介するプロキシ装置であって、

前記外部ネットワーク上の装置から前記内部ネットワーク上の装置に送信される文書に付された電子署名を検証する署名検証部と、

前記署名検証部による検証が成功した場合、その文書からその電子署名を削除し、その文書に対して当該署名プロキシ装置の内部ネットワーク用の署名鍵を用いて電子署名を付与し直して、前記内部ネットワーク上の前記装置へと送信する署名変換部と、

を備える署名プロキシ装置。

【請求項２０】　内部ネットワークと外部ネットワークとの間に介在するプロキシ装置において、該内部ネットワーク上の装置と前記外部ネットワーク上の装置との間で文書のやりとりを媒介する方法であって、

前記外部ネットワーク上の装置から前記内部ネットワーク上の装置に送信される文書に付された電子署名を検証し、

この検証が成功した場合、その文書からその電子署名を削除し、

その電子署名を削除した前記文書に対して当該署名プロキシ装置の内部ネットワーク用の署名鍵を用いて電子署名を付与し直し、

前記内部ネットワーク用の署名鍵を用いて電子署名を付与し直した前記文書を、前記内部ネットワーク上の前記装置へと送信する、

方法。

【請求項２１】　内部ネットワークと外部ネットワークとの間に介在し、該内部ネットワーク上の装置と前記外部ネットワーク上の装置との間で文書のやりとりを媒介するコンピュータのプログラムであって、

コンピュータを、

前記外部ネットワーク上の装置から前記内部ネットワーク上の装置に送信され

る文書に付された電子署名を検証する署名検証部と、

前記署名検証部による検証が成功した場合、その文書からその電子署名を削除し、その文書に対して当該署名プロキシ装置の内部ネットワーク用の署名鍵を用いて電子署名を付与し直して、前記内部ネットワーク上の前記装置へと送信する署名変換部と、

して機能させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワーク上に存在する処理装置を連携させた連携処理を実現するための技術に関し、特に連携処理におけるセキュリティ技術に関する。

【０００２】

【従来の技術及び発明が解決しようとする課題】

スキャナ、ファクシミリ装置、プリンタ、複写機、及びそれらの機能を統合した複合機をＬＡＮ（ローカルエリアネットワーク）に接続し、パーソナルコンピュータやメールサーバなどの情報処理装置と連携させ、オフィス作業用の各種サービスを提供するワークフローシステムが提案されている。

【０００３】

また近年、インターネット上に散在する各種ウェブアプリケーションを連携させる技術が提案されている。インターネット上にある多様な提供者が提供するアプリケーションサービスを連結して１つのシステムを構成できると、様々な既存サービスを利用することができるのでシステム開発コストが大幅に低減できると期待されている。また、このような連携的なサービスを実現するための共通の基盤としてＸＭＬ(eXtensible Markup Language)等の言語が注目されている。

【０００４】

また、従来のワークフローシステムとしては、特許文献１や特許文献２、特許文献３に示されるものが知られている。

【０００５】

ワークフローシステムでは、フローを構成する各処理装置に対するサービスの

要求は、指示データを処理装置から処理装置へと順に受け渡すことにより行われる。ここで、指示データの改ざんや、なりすましなどの危険性があると、処理装置側が要求するセキュリティレベルを満足できない場合が出てくる。

【０００６】

これは、ワークフローにイントラネットワーク外の処理装置を組み込む場合に顕著な問題となる。ワークフローに組み込まれる外部処理装置としては、例えば、第三者機関としてデータの存在証明を行うタイムスタンプサーバや、サービス提供者に代わって代金徴収を行う代金回収サーバ（例えばクレジットカード会社の決済処理装置）など、様々なものがある。

【０００７】

このようなデータの改ざんやなりすまし等の防止にはＰＫＩ（公開鍵基盤）の電子署名が利用されており、これを処理装置間の指示データの通信に利用することが考えられる。

【０００８】

しかしながら、イントラネットワークの内外に存在する処理装置でデータを受け渡す場合には、電子署名の検証が困難となる。これは以下のような理由によるものである。

【０００９】

一概に認証局（ＣＡ:Certificate Authority。認証機関とも言う）といっても、政府やVerisign社などが設置する公的な信用力のある認証局から、企業が社内や部内に設ける認証局まで、様々なレベルがある。企業のイントラネット上にある処理装置やインターネット上にある処理装置を組み合わせてワークフローを構築する場合、各処理装置が受けている公開鍵証明書の発行元ＣＡは様々に異なると想定される。ここで、ＣＡは、ウェブサーバやＬＤＡＰ（Lightweight Directory Access Protocol）サーバなどにより各ユーザ（ＰＫＩの側面では処理装置もユーザである）の公開鍵証明書を公開しており、電子署名を検証する側はこれらサーバから検証に必要な公開鍵証明書を取得することとなる。ここで、社内（イントラネット内）の処理装置が社内ＣＡの公開鍵証明書の秘密鍵を用いて電子署名を行った指示データを社外（イントラネット外）の処理装置に送信した場合

、社外の処理装置は、ファイヤーウォールに阻まれて社内ＣＡから公開鍵証明書を得ることができない場合がある。

【００１０】

また、仮に社外の装置から社内ＣＡ発行の公開鍵証明書が取得できるようにした場合、次のような問題がある。すなわち、社内ＣＡが発行する公開鍵証明書には当該証明書の所有者の名称や所属等の情報が含まれる場合が多く、これがそのまま社外に流れると、社内の組織構成が知られてしまうという問題がある。

【００１１】

なお、特許文献４には、異なるイントラネット内にある装置間での文書のやりとりの際の電子署名のための、署名プロキシサーバが開示されている。この署名プロキシサーバは、イントラネット内の装置が発した文書に対し、その装置に代わって電子署名を付与すると共に、外部からイントラネット内の装置への文書の電子署名の検証を代行する。

【００１２】

特許文献４では、イントラネット内の装置内の文書に対する電子署名については考慮が払われていない。特許文献４のシステムでは、イントラネット内の装置は自らの発したデータに対して電子署名を施さず、署名プロキシサーバはイントラネット内の装置から外部に送られるデータに対し、真正性の検証を行うことなく電子署名を付している。

【００１３】

【特許文献１】

特開平０８－１２３７４４号公報

【特許文献２】

特開２００２－０９９６８６号公報

【特許文献３】

特開２００１－２８２９７０号公報

【特許文献４】

特開２００２－１６４８８４号公報

【００１４】

【課題を解決するための手段】

本発明のある側面では、ジョブ処理を指示する処理記述が記述された指示データ、またはジョブ処理の対象となる被処理データをジョブ処理装置に送信し、ジョブ処理を実行させる情報処理装置であって、第１の認証機関により認証された第１の署名鍵と、第２の認証機関により認証された第２の署名鍵のいずれで指示データまたは被処理データに署名するかを切り換える切換部と、前記切換部により切り換えられた署名鍵で、前記指示データまたは前記被処理データに署名を施す署名部と、前記署名部により署名された指示データまたは被処理データを前記ジョブ処理装置に向けて送信する送信部と、を備える情報処理装置を提供する。

【００１５】

本発明の別の側面では、自装置が属するネットワークの内部用と外部用にそれぞれ別の署名鍵を有する鍵記憶部と、各ジョブ処理装置に対する処理指示と各ジョブ処理装置の次のジョブ処理装置とを示したフロー指示データを受信する受信部と、前記受信部で受信したフロー指示データに付与された電子署名を検証する署名検証部と、前記署名検証部による検証が成功した場合に、前記フロー指示データ内から自装置が実行すべき処理指示を識別し、その処理指示に従って処理を実行する処理部と、前記処理部により処理を実行した場合に、前記受信したフロー指示データを基に、自装置の次のジョブ処理装置に送信する出力フロー指示データを作成する指示データ作成部と、前記次のジョブ処理装置が前記ネットワーク内の装置か否かを判定する判定部と、前記次のジョブ処理装置が前記ネットワーク内の装置である場合には前記内部用の署名鍵を用い、そうでない場合は前記外部用の署名鍵を用いて、前記出力フロー指示データに電子署名を付与する署名処理部と、前記署名処理部で電子署名が付与された出力フロー指示データを前記次のジョブ処理装置に送信する送信部と、を備えるジョブ処理装置を提供する。

【００１６】

また、本発明の別の側面では、各ジョブ処理装置に対する処理指示と各ジョブ処理装置の次のジョブ処理装置とを示したフロー指示データをそれら各ジョブ処理装置間で順に受け渡しながら、それら各ジョブ処理装置がそれぞれ自装置に対する処理指示を順に実行することでサービスを実現するシステムのために、前記

フロー指示データを作成する指示データ作成装置であって、当該指示データ作成装置が属するネットワークの内部用の署名鍵と外部用の署名鍵とを有する鍵記憶部と、前記サービスのためのジョブ処理装置群の中に、前記ネットワークの外部にあるジョブ処理装置が含まれているか否かを判定する判定部と、前記サービスのためのジョブ処理装置群の中に前記ネットワークの外部にある装置が含まれていると前記判定部で判定された場合は前記外部用の署名鍵を用い、そうでない場合は前記内部用の署名鍵を用いて前記フロー指示データに電子署名を付与する署名処理部と、前記署名処理部で電子署名が付与されたフロー指示データを前記サービスにおけるジョブ処理装置群の中の最初のジョブ処理装置に送信する送信部と、を備える指示データ作成装置を提供する。

【００１７】

本発明の更に別の側面では、内部ネットワークと外部ネットワークとの間に介在し、該内部ネットワーク上の装置と前記外部ネットワーク上の装置との間で文書のやりとりを媒介するプロキシ装置であって、前記内部ネットワーク上の装置から前記外部ネットワーク上の装置に送信される文書に付された電子署名を検証する第１署名検証部と、前記第１署名検証部による検証によりその文書に付された電子署名が内部ネットワーク用の署名鍵を用いたものであることが分かった場合は、前記文書からその電子署名を削除し、前記文書に対して当該署名プロキシ装置の外部ネットワーク用の署名鍵を用いて電子署名を付与し直して、前記外部ネットワーク上の前記装置へと送信する第１署名変換部と、を備えるプロキシ装置を提供する。

【００１８】

本発明の更に別の側面では、内部ネットワークと外部ネットワークとの間に介在し、該内部ネットワーク上の装置と前記外部ネットワーク上の装置との間で文書のやりとりを媒介するプロキシ装置であって、前記外部ネットワーク上の装置から前記内部ネットワーク上の装置に送信される文書に付された電子署名を検証する署名検証部と、前記署名検証部による検証が成功した場合、その文書からその電子署名を削除し、その文書に対して当該署名プロキシ装置の内部ネットワーク用の署名鍵を用いて電子署名を付与し直して、前記内部ネットワーク上の前記

装置へと送信する署名変換部と、を備える署名プロキシ装置を提供する。

【００１９】

【発明の実施の形態】

以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて説明する。

【００２０】

まず図１を参照して、本発明が適用されるサービス提供システムのシステム構成パターンの別の一例を説明する。

【００２１】

このシステムは、指示入力装置１０と複数のアプリケーションサーバ２０とから構成されている。

【００２２】

アプリケーションサーバ２０は、他の装置からの要求に応じて所定の処理サービスを提供するサーバである。例えば、サーバ２０の例としては、文書データベースサーバや、メールサーバ、画像データに対して色変換や回転などの操作を施す画像処理サーバ等を挙げることができる。サーバ２０は、そのような処理サービスを例えばウェブアプリケーションサービス等の形で提供する。

【００２３】

指示入力装置１０は、このシステムに対するユーザの処理指示を入力するための装置である。ユーザは、指示入力装置１０に対し、上述のような連携サービスの実行指示を入力することができる。指示入力装置１０は、例えばパーソナルコンピュータに、ユーザから本システムへの指示の入力を受け付けるためのユーザインタフェースプログラムを組み込んだものでよい。しかしながら、オフィスにおける文書処理サービスを想定すると、情報処理機能や通信機能に加え、紙文書を読み取って電子データ化する機能をも備えるデジタル複合機を指示入力装置１０として用いることが好適である。なお、デジタル複合機は、スキャナ、プリンタ、複写機、ファクシミリ送受信、ネットワーク通信等の機能を併せ持つ装置である。

【００２４】

このシステムでは、指示入力装置１０に対しユーザが所望の連携サービスの実行指示を入力する。指示入力装置１０は、この指示入力に応じ、その連携サービスの内容を示す指示データ（以下「フロー指示書」と呼ぶ）を作成する。

【００２５】

このフロー指示書３０は、この連携サービスのために各サーバ２０が実行すべき処理内容の記述（個別指示書と呼ぶ）と、それら各処理内容の実行順序の情報を含む。このようなフロー指示書の具体的な構造としては、各サーバ２０への個別指示書３２－１～３２－３を、連携サービスにおける当該処理の実行の順序に従って並べた構造を用いることができる。ここで、各サーバ２０宛の個別指示書３２には、当該サーバ２０の名称（サービス名と呼ぶ）などが記述されており、これにより各サーバ２０はフロー指示書３０の中から自分が処理すべき個別指示書３２を識別することができる。サービス名は、例えばＵＲＬ(Universal Resource Locator)等の形で記述される。また、個別指示書３２は処理順に並んでいるので、各サーバ２０は、自分宛の個別指示書３２の次の個別指示書３２のサービス名などの記述から、自分の次に処理を実行するサーバ２０を識別することができる。なお、個別指示書３２の中に、当該サーバ２０の次に処理を行うサーバ２０（すなわち、次にフロー指示書を渡すべき相手）を示す記述を組み込んでももちろんよい。これにより、各サーバ２０は、フロー指示書３０から自分宛の処理記述を認識し、それに応じた処理を実行し、その処理の後、次のサーバ２０にフロー指示書３０をまわすことができる。

【００２６】

図１の例では、このようなフロー指示書３０が指示入力装置１０から連携サービスの最初のサーバ２０－１に対して送信されることで、連携サービス処理が開始される。これを受け取ったサーバ２０－１は、フロー指示書３０から自分宛の個別指示書３２－１を識別し、これに従って処理を実行する。そしてサーバ２０－１は、そのフロー指示書３０から自分宛の個別指示書３２－１を削除して新たなフロー指示書３０ａを作成し、これをフロー中の次のサーバ２０－２に送信する。フロー指示書３０ａを受信したサーバ２０－２も同様に動作し、そのフロー指示書３０ａから自分宛の個別指示書３２－２を削除してフロー指示書３０ｂを

作成し、次のサーバ２０－３に送る。

【００２７】

このようなシステムでは、各サーバ２０が自分の受け取ったフロー指示書３０，３０ａ，３０ｂ（以下、フロー指示書３０と総称）の真正性（改ざんがなされていないなど）を検証できるようにするための仕組みとして、電子署名を用いる。すなわち、指示入力装置１０や各サーバ２０は、送信しようとするフロー指示書３０に対して自装置の電子署名を付与することとし、フロー指示書３０を受け取ったサーバ２０はその署名を検証することで、そのフロー指示書３０の真正性を判定する。

【００２８】

このようなシステムにおいて、例えばサーバ２０－１及び２０－３が指示入力装置と同じ会社内（すなわち当該会社のイントラネット内）に存在し、サーバ２０－２が社外（イントラネット外）に存在するとする。この場合、サーバ２０－１からサーバ２０－２に送られるフロー指示書３０ａが、サーバ２０－１の属する会社の社内の認証局（ＣＡ）が発行した公開鍵証明書に対応する秘密鍵により署名されていると、前述のように、社外のサーバ２０－２はその署名の検証に必要な公開鍵証明書を社内のＣＡから取得できないなどの問題が生じる。

【００２９】

そこで、本実施形態では、各サーバ２０に対して、当該サーバ２０の属する会社（あるいは部門）のＣＡ（以下、社内ＣＡと略称する）と、政府やVerisign社などの公的なＣＡ（以下、公的ＣＡと略称する）の両方から公開鍵証明書を受けておく（証明書に対応する鍵ペアは、社内ＣＡと公的ＣＡとで同じである必要はない）。そして、各サーバ２０は、次のサーバ２０に対し送るフロー指示書３０に対し電子署名を行う際に、当該次のサーバ２０が社内か社外かを判定し、社内の場合は社内ＣＡの公開鍵証明書に対応する秘密鍵を用いて電子署名を施し、社外の場合は公的ＣＡの公開鍵証明書に対応する秘密鍵を用いて電子署名を施す。すなわち、この例では、各サーバ２０が社内用と社外用の２種類の電子署名を行うことができ、フロー指示書３０を送る宛先の装置が社内か社外かに応じてその両者を使い分ける。

【００３０】

ここで、社内ＣＡは、会社や部門などに所属する限定された利用者（個人だけでなく、人のグループや装置の場合などもある）の公開鍵を認証するのに対し、公的ＣＡは、不特定多数の利用者の公開鍵を認証する。

【００３１】

図２は、このシステムにおけるサーバ２０の機能ブロック図である。この図では、サーバ２０が持つ機能のうち、電子署名に関連する部分を重点的に示している。サーバ２０は、これら以外の機能を含み得る。

【００３２】

図２において、ネットワークＩ／Ｆ（インタフェース）部２０２は、当該サーバ２０とローカルエリアネットワークとのデータ通信を制御する手段である。

【００３３】

指示書分割／統合部２０４は、直前のサーバ２０からネットワークＩ／Ｆ２０２を介して受信したフロー指示書３０の分割と、次のサーバ２０に送信するフロー指示書３０の組み立てを行う手段である。受信したフロー指示書３０の分割は、大まかに言えば、処理内容を記述した部分と電子署名について記述した部分とに分ける処理である。これを、図３の具体的なフロー指示書の例を用いて説明する。

【００３４】

図３は、ＸＭＬ-signature(eXtensible Markup Language - signature;RFC3275）に従って記述したフロー指示書の例である。このフロー指示書は、各サーバ２０の処理内容を記述した処理内容要素３１０と、この処理内容要素３１０に対する電子署名の情報を記述した署名要素３２０から構成されている。

【００３５】

処理内容要素３１０は、各サーバ２０宛の個別指示書３１２、３１４を含んでいる。各個別指示書３１２、３１４には、当該指示書の宛先を示すサービス名３１２２，３１４２と、該宛先サービスが実行すべき処理の種類を示す処理名３１２４，３１４４と、その処理の際のパラメータ３１２６とを含む。

【００３６】

署名要素３２０は、該フロー指示書３０の電子署名に用いたアルゴリズムや署名対象要素（この場合は処理内容要素３１０）のハッシュ値等を示した署名情報要素３２２と、署名対象要素に対してそのアルゴリズムにより求めた署名値を示す署名値要素３２４と、その電子署名の検証に用いるべき公開鍵を特定するための情報を記述した鍵情報要素３２６を含む。鍵情報要素３２６には、電子署名の値の計算に用いた秘密鍵に対応する公開鍵証明書を特定するのに必要な情報が含まれる。なお、署名要素３２０内の各要素の詳細については上述のＸＭＬ-signature規格を参照されたい。

【００３７】

指示書分割／統合部２０４は、前段のサーバ２０から受け取ったこのような構成を持つフロー指示書３０を、処理内容要素３１０と署名要素３２０に分割すると共に、署名要素３２０を更に、署名情報要素３２２及び署名値要素３２４と、鍵情報要素３２６とに分割する。この分割の後、処理内容要素３１０は指示書処理部２１２及び署名検証部２１０へ、鍵情報要素３２６は検証鍵選択部２０８へ、署名情報要素３２２及び署名値要素３２４は署名検証部２１０へ、とそれぞれ送られる。

【００３８】

鍵保管部２０６は、次のサーバに送るべきフロー指示書３０等への電子署名付与に用いる自装置の秘密鍵や、受信したフロー指示書３０の署名検証に用いる他のサーバ２０の公開鍵を保管している。ここで、署名用の秘密鍵としては、社内ＣＡにより証明された社内用のものと、公的ＣＡにより証明された社外用のものとを保管している。これら両者は、鍵の値自体は同一でもよいが、対応する公開鍵証明書が社内用と社外用とで異なる。

【００３９】

検証鍵選択部２０８は、指示書分割／統合部２０４から送られてきた鍵情報要素３２６の情報が示す公開鍵を鍵保管部２０６から取得し、署名検証部２１０に渡す。

【００４０】

署名検証部２１０は、指示書分割／統合部２０４から受け取った処理内容要素

３１０、署名情報要素３２２及び署名値要素３２４と、検証鍵選択部２０８から受け取った公開鍵とを用いて、当該フロー指示書３０に付された電子署名を検証する。この検証処理では、署名値要素３２４に示される署名値を検証鍵選択部２０８から受け取った公開鍵で復号すると共に（このとき署名情報要素３２２に示されるアルゴリズムを用いる）、処理内容要素３１０のハッシュ値を求め、上記復号の結果とこのハッシュ値とが一致した場合には、検証が成功したとする。なお、この検証が失敗した場合は、処理内容要素３１０又は署名要素３２０のいずれかに改ざんが加えられている可能性があるので、サーバ２０は所定のエラー処理を実行する。

【００４１】

指示書処理部２１２は、フロー指示書３０に対する処理を実行する手段である。署名検証部２１０による検証が成功した場合、指示書処理部２１２は、そのフロー指示書３０の中から自分宛の個別指示書３２を識別し、その個別指示書３２に示される処理内容を実行する。例えば、フロー指示書３０中の当該サーバ２０宛の個別指示書３２に対し、画像データに対する解像度変換の実行指示が示されていた場合、そのサーバ２０は、そのフロー指示書３０と共に受信した画像データ（この画像データがその指示書に対応する処理の処理対象である）に対し、その解像度変換処理を施す。

【００４２】

なお、図１の例のように、各サーバ２０が自分の処理が終わるごとに自分宛の個別指示書３２を削除して次のサーバ２０に渡す構成の場合、受信したフロー指示書３０の先頭にある個別指示書３２が自サーバ宛の個別指示書である。もちろんこの他にも、サービス名称の記述３１２２などを参照して自サーバ宛の個別指示書を識別することもできる。

【００４３】

また、指示書処理部２１２は、署名検証部２１０の検証が失敗した場合は、処理内容要素３１０又は署名要素３２０のいずれかに改ざんが加えられている可能性があるので、フロー指示書３０に対する処理は中止し、所定のエラー処理を実行する。

【００４４】

署名検証が成功し、指示書処理部２１２による処理がなされると、次に指示書作成部２１４が、直前のサーバ２０から受信したフロー指示書３０から自サーバ宛の個別指示書３２を取り除いて、次のサーバ２０宛のフロー指示書３０（この指示書を出力フロー指示書と呼ぶ）の処理内容要素３１０を作成する。なお、当該サーバ２０の処理内容によって次のサーバ２０やそれ以降のサーバ２０の処理に対するパラメータが決まることもあるので、その場合は出力フロー指示書の処理内容要素３１０にはその処理の結果に基づき決定したパラメータが記述されることになる。

【００４５】

署名鍵選択部２１６は、その出力フロー指示書の処理内容要素３１０に対する電子署名に用いる署名鍵を選択する。ここで、鍵保管部２０６には、当該サーバ２０の署名鍵（秘密鍵）が社内用と社外用の２種類保管されているので、署名鍵選択部２１６はこれら２種類のうちから使用するものを選択する。この選択では、その出力フロー指示書の宛先であるサーバ２０が社内、社外のいずれであるかを判定し、その判定に応じ、宛先サーバ２０が社内であれば社内用の署名鍵を、社外であれば社外用の署名鍵を、それぞれ選択する。宛先のサーバ２０が社内か社外かは、その宛先サーバ２０への個別指示書３１４のサービス名に示されるＵＲＬに基づき判別する。このＵＲＬに基づく判定は、例えば、サービス名のＵＲＬに対応するＩＰアドレスを所定のネームサーバに問い合わせ、その結果得られたＩＰアドレスに基づき社内か社外かを判定するなどの方法で行うことができる。署名鍵選択部２１６は、選択した署名鍵をかぎ保管部２０６から読み出し、署名作成部２１８に渡す。

【００４６】

署名作成部２１８は、指示書作成部２１４から受け取った処理内容要素３１０に対する電子署名を、署名鍵選択部２１６から取得した署名鍵を用いて作成する。この署名作成処理では、その処理内容要素３１０についてのハッシュ値を計算し、そのハッシュ値に対してその署名鍵を作用させることで署名値を計算する。そして、その署名値の計算に用いたアルゴリズムを記述した署名情報要素３２２

と、その署名値を含む署名値要素３２４と、使用した署名鍵に対応する公開鍵証明書を示す鍵情報要素３２６とを作成し、これを指示書分割／統合部２０４に渡す。

【００４７】

指示書分割／統合部２０４は、署名作成部２１８で作成された署名情報要素３２２，署名値要素３２４及び鍵情報要素３２６を、指示書作成部２１４で作成された処理内容要素３１０に付加することで、出力フロー指示書を作成する。作成された出力フロー指示書は、ネットワークＩ／Ｆ部２０２を介して、宛先のサーバ２０に送信される。

【００４８】

以上説明したように、本実施形態の構成では、連携サービスの部分的な処理を実行するサーバ２０が、次に処理を実行するサーバ２０が社内か社外かを判定し、社外の場合は公的なＣＡが発行した公開鍵証明書で検証可能な電子署名を付する。したがって、社外のサーバ２０が社内のサーバ２０からフロー指示書を受け取った場合には、公的ＣＡからその社内サーバ２０の公開鍵証明書を取得して署名検証を行うことができる。また、社内ＣＡの公開鍵証明書に含まれる組織構成情報などの社内情報が社外のサーバ２０に漏れることも防止できる。

【００４９】

また、本実施形態のサーバ２０は、次に処理を実行するサーバ２０が社内のサーバである場合、社内ＣＡの公開鍵証明書で検証できる電子署名をフロー指示書に施すので、次のサーバ２０（社内）は、インターネット上の公的ＣＡから公開鍵証明書を取得する必要なく、簡便にその署名を検証することができる。

【００５０】

以上では、社内か社外かの２分法で署名鍵を選択したが、この２分法はあくまで一例にすぎない。この他にも、同じ社内でもある部門内か否かといった２分法で署名鍵を使い分けることもできる。

【００５１】

また、以上の例では、フロー指示書３０に付する電子署名を例にとったが、この他に、フロー指示書に付随して送信するデータ（例えば、次段の装置での処理

の対象となるデータ）にも、同様の仕組みで、その送信先に応じた電子署名を施すことができる。

【００５２】

また、以上に説明した電子署名方式は、図４に示すような構成のシステムにも適用できる。

【００５３】

図４のシステムは、指示入力装置３０と各サーバ２０の他に、フロー制御装置２５を含んでいる。このフロー制御装置２５は、このシステムにおける各サーバ２０の処理の実行を制御する装置である。すなわち、フロー制御装置２５は、指示入力装置１０で作成されたフロー指示書３０を受け取り、このフロー指示書３０から各サーバ２０への個別指示書３２を取り出し、これら各個別指示書３２を各サーバ２０に対して処理順に送信していく。各サーバ２０は、受け取った個別指示書３２に従って処理を実行し、その処理が終了すると、処理結果のデータをフロー制御装置２５に返す。これを受け取ったフロー制御装置２５は、次のサーバ２０宛に個別指示書３２を送る。このような手順の繰り返しにより、複数のサーバ２０の連携により１つのサービスフローを実現できる。

【００５４】

ここで、フロー制御装置２５は、指示入力装置１０と同じ社内のイントラネットワークに接続されているものとする。

【００５５】

このような図４のシステムにおいて、フロー制御装置２５は、社内用の公開鍵証明書を受けた署名鍵と社外用の公開鍵証明書を受けた署名鍵とを備えている。そしてフロー制御装置２５は、指示入力装置１０から受け取ったフロー指示書３０の電子署名を検証し、その署名が指示入力装置１０の正しい署名であると判定すると、そのフロー指示書３０の処理内容要素３１０から各サーバ２０宛の個別指示書３２（３１２，３１４等）を取り出し、順に送信していく。この送信の際、フロー制御装置２５は、個別指示書３２の宛先のサーバ２０が社内のイントラネットワーク上の装置か否（社外）かを判別し、社内であれば社内用の証明書に対応する署名鍵で、社外であれば社外用の証明書に対応する署名鍵で、その個別

指示書３２に対して電子署名を施す。これにより、その個別指示書３２を受け取ったサーバ２０が社外のサーバであっても社内のサーバであっても、スムーズにその署名の検証を行うことができる。

【００５６】

なお、この構成においても、指示入力装置１０からのフロー指示書３０に含まれる社内の指示入力装置１０の電子署名が社外のサーバ２０に伝送されることはない。

【００５７】

以上に示したシステムは、個々のサーバ２０が次にフロー指示書３０を送る相手のサーバ２０が社内か、社外かを判別し、それに応じた署名鍵を用いて電子署名を行った。しかしながら、これは本発明の実施形態の１つに過ぎない。上記実施形態の変形例として次のようなものがある。

【００５８】

すなわち、上記実施形態では、各サーバ２０が次のサーバ２０へ渡すフロー指示書３０を作成し、それに自サーバの電子署名を施したのに対し、この変形例では、指示入力装置１０が作成し、電子署名を施したフロー指示書をそのままサーバ２０から次のサーバ２０へと受け渡す。このような構成の場合、指示入力装置１０が、フロー指示書に付与する電子署名のために、社内用、社内用のいずれの公開鍵証明書に対応する署名鍵を用いるかが問題となる。このため、この変形例の指示入力装置１０は、ユーザから要求された連携サービスのために使用する各サーバ２０が社内の装置か社外の装置かをそれぞれ判定し、その中に一つでも社外の装置が含まれていれば、社外用の署名鍵を用いてフロー指示書に署名を施す。逆に、その連携サービスに使用するサーバ２０がすべて社内のものである場合は、社内用の署名鍵を用いて電子署名を施す。

【００５９】

図５は、この変形例の指示入力装置１０の構成を示す機能ブロック図である。この構成において、操作表示部１０２は、ユーザの指示入力のためのユーザインタフェース画面を表示すると共に、その画面に応じたユーザの入力を受け取る手段である。ユーザからの連携サービスの実行指示は、この操作表示部１０２から

入力される。この実行指示の入力のために、例えば操作表示部１０２は選択可能な連携サービスの名前のリストを画面表示し、ユーザに所望のものを選択させ、必要に応じて処理パラメータを入力させる。処理パラメータとしては、例えば電子メール送信サーバに対するメール送信先アドレスなどを挙げることができる。ここで、サービスＤＢ（データベース）１０４には、各連携サービスの名前に対応づけて、当該連携サービスに対応するフロー指示書３０のひな形を有している。このひな形は、図３に示した署名付きのフロー指示書のうち、処理内容要素３１０に該当する部分のひな形である。処理内容要素３１０には、使用する各サーバ２０を特定するサービス名３１２２、３１４２などの情報が含まれている。

【００６０】

指示書作成部１０６は、ユーザが選択した連携サービスとそのパラメータを操作表示部１０２から受け取り、その連携サービスに対応するフロー指示書のひな形をサービスＤＢ１０４から取得し、これに対してそのパラメータを代入することで、フロー指示書の処理内容要素３１０を完成させる。作成された処理内容要素３１０は、指示書統合部１１４と署名作成部１１２に提供される。また、指示書作成部１０６は、処理内容要素３１０に含まれる、各サーバ２０のサービス名３１２２，３１４２の情報を、署名鍵選択部１１０に渡す。

【００６１】

鍵保管部１０８は、フロー指示書３０への電子署名のための鍵として、社内ＣＡが発行した公開鍵証明書に対応する鍵と、公的ＣＡが発行した公開鍵証明書に対応する鍵の２種類を備えている。

【００６２】

署名鍵選択部１１０は、指示書作成部１０６から提供された、連携サービスにおいて使用する各サーバ２０の情報に基づき、それらサーバ２０の中に社外のものが含まれるか否かを判定し、１つでも含まれれば社外用の署名鍵を、１つも含まれなければ社内用の署名鍵を選択し、これを鍵保管部１０８から取り出して署名作成部１１２に渡す。

【００６３】

署名作成部１１２は、指示書作成部１０６から受け取った処理内容要素３１０

と、署名鍵選択部１１０から受け取った署名鍵とを用いて、上述と同様にして署名情報要素３２２，署名値要素３２４，及び鍵情報要素３２６を作成し、これを指示書統合部１１４に渡す。

【００６４】

指示書統合部１１４は、署名作成部１１２で作成された署名情報要素３２２，署名値要素３２４及び鍵情報要素３２６を、指示書作成部１０６で作成された処理内容要素３１０に付加することで、出力フロー指示書を作成する。作成された出力フロー指示書は、ネットワークＩ／Ｆ部１０２を介して、連携サービスの最初のサーバ２０に送信される。

【００６５】

以降、各サーバ２０は、受け取ったフロー指示書３０にある指示入力装置１０の電子署名を検証し、この検証が成功すれば、その指示書３０の中から自装置宛の個別指示書３２を識別し、その個別指示書３２に示された処理を実行した後、受け取ったフロー指示書３０をそのまま次のサーバ２０に送信する。

【００６６】

次に、更なる変形例を説明する。この変形例では、図６に示すように、指示入力装置１０や各サーバ２０が接続された社内のＬＡＮ５０（あるいはイントラネット）に、署名プロキシ装置４０を設ける。署名プロキシ装置４０は、社内ＣＡと公的ＣＡからそれぞれ公開鍵証明書を受けている。ここで、アプリケーションサーバ６０が社外（イントラネット外）に存在するものとする。

【００６７】

このシステムでは、社内のＬＡＮ５０上の指示入力装置１０や各サーバ２０は、社内ＣＡが発行した公開鍵証明書に対応する秘密鍵のみを持っていればよく、次のサーバ２０に送るフロー指示書３０にはその社内用の秘密鍵を用いて電子署名を行う。各サーバ２０の処理は、署名に用いる鍵の選択を行わない（すなわち常に社内用の署名鍵を用いる）点以外は、図２に示した実施形態のサーバ２０の処理と同様でよい。

【００６８】

社内の指示入力装置１０や各サーバ２０には、フロー指示書３０をイントラネ

ット外に送信する際に用いるプロキシサーバとして、署名プロキシ装置４０のＩＰアドレスや名前が設定されている。指示入力装置１０や各サーバ２０は、次のサーバ２０に自分の署名付きのフロー指示書３０を送る場合に、送り先のサーバが社内か社外かを判別し、社内の場合はそのサーバにその署名付きの指示書３０を直接送信し、社外の場合はその署名付きの指示書３０を署名プロキシ装置４０に送信する。図６の例では、サーバ２０－２は、次のサーバ６０が社外の装置であると判別し、自分の署名付きのフロー指示書３０を署名プロキシ装置４０に送っている。

【００６９】

これを受け取った署名プロキシ装置４０は、そのフロー指示書３０の署名を検証し、その検証が成功すれば、そのフロー指示書３０からサーバ２０－２の電子署名（社内用の署名鍵を用いている）の署名要素３２０を削除し、その結果現れた処理内容要素３１０に対し、当該署名プロキシ装置４０の社外用の公開鍵証明書に対応する秘密鍵を用いて電子署名を施すことでフロー指示書３５を作成し、社外の宛先サーバ６０に送信する。

【００７０】

また、社内のサーバ２０は、社外のサーバ６０から直接フロー指示書を受け取ることはない。社外のサーバ６０から社内のサーバ２０－３宛のフロー指示書３７は、いったん署名プロキシ装置４０に受信される。この場合署名プロキシ装置４０は、そのフロー指示書３７に付された電子署名を検証し、この検証が成功した場合は、そのフロー指示書３７から社外サーバ６０の電子署名の署名要素３２０を削除し、その結果現れた処理内容要素３１０に対し、当該署名プロキシ装置４０の社内用の公開鍵証明書に対応する秘密鍵を用いて電子署名を施すことで社内用のフロー指示書３０を作成し、宛先のサーバ２０－３に送信する。

【００７１】

このように署名プロキシ装置４０は、社内から社外への指示書、及び社外から社内への指示書について、電子署名の付け替え処理を行う。このような付け替え処理によれば、社内の指示入力装置１０やサーバ２０は、社内ＣＡからのみ公開鍵証明書を受け、宛先が社内か社外かによらず社内用の署名鍵を用いて指示書に

電子署名を行っていればよい。指示書が社外に出る場合は、署名プロキシ装置４０がその署名を社外用に付け替える。これにより、社内のサーバ２０同士の間でのフロー指示書３０の改ざん等の有無を検知できると共に、社内・社外間でのフロー指示書の改ざん等の有無を検知することもできる。また、社外のサーバ６０は、署名プロキシ装置４０の社外用の公開鍵証明書を公的ＣＡから入手すれば、指示書３５の署名が検証できるので、署名検証が容易である。

【００７２】

また、このシステムでは、社外サーバ６０からの署名付き指示書３７は、署名プロキシ装置４０により署名検証され、それが成功した場合には、フロー指示書３７の電子署名が署名プロキシ装置４０の社内用の電子署名に付け替えられた上で、宛先の社内サーバ２０－３に渡される。したがって、このシステムでは、社内のサーバ２０は、社内ＣＡが発行した公開鍵証明書を用いた署名検証を行う能力を持てばよく、社外のＣＡの公開鍵証明書にまで対応する必要がない。

【００７３】

署名プロキシ装置４０の構成の一例を、図７を用いて説明する。

【００７４】

この装置４０において、指示書分割／統合部４０４は、ネットワークＩ／Ｆ部４０２を介してフロー指示書３０を受け取った場合、そこから取り出した処理内容要素３１０を署名検証部４１０及び署名変換制御部４１２へ、署名情報要素３２２及び署名値要素３２４（図３参照）を署名検証部４１０に、鍵情報要素３２６を検証鍵選択部４０８へ、それぞれ提供する。検証鍵選択部４０８は、その鍵情報要素３２６が示す公開鍵を鍵保管部４０６から取り出し、署名検証部４１０に渡す。署名検証部４１０は、その公開鍵を用いて、図２の実施形態と同様の署名検証処理を実行する。この検証結果（成功か失敗か）は、署名変換制御部４１２に渡される。

【００７５】

署名変換制御部４１２は、そのフロー指示書３０が社内のサーバ２０からのものであれば、その指示書３０の署名を社外用のものに付け替えるよう、署名鍵選択部４１６に指示する。またフロー指示書３０が社外のサーバ６０からのもので

あれば、その指示書３０の署名を社内用のものに付け替えるよう、署名鍵選択部４１６に指示する。なお、フロー指示書３０が社内のサーバ２０からのものか社外のサーバ６０からのものかの判別は、署名検証部４１０で署名検証に用いた公開鍵が社内ＣＡで証明を受けたものか社外のＣＡで証明を受けたものかで判別できる。また更に別の例として、ネットワークＩ／Ｆ部４０２からそのフロー指示書３０の送信元のＵＲＬやＩＰアドレスの情報を受け取り、これに従って判定を行ってもよい。

【００７６】

なお、以上では、署名プロキシ装置４０には、社内から社外への指示書か、社外から社内への指示書しか到来しないものとして説明しているが、社内から社内への指示書も署名プロキシ装置４０を経由する可能性がある場合は、送信元だけでなく送信先も検査する。すなわち、署名変換制御部４１２は、社内から社外への指示書や、社外から社内への指示書については上述の署名付け替えを行い、社内から社内への指示書についてはそのような付け替えを行わないと判定する。ここで、フロー指示書３０の送信先は、フロー指示書３０の処理内容要素３１０の先頭の個別指示書のサービス名３１２２に示されたＵＲＬや、ネットワークＩ／Ｆ部４０２から受け取った宛先ＩＰアドレスなどから判別できる。

【００７７】

署名鍵選択部４１６は、署名鍵変換制御部４１２の指示に応じた当該プロキシ装置４０の署名鍵（社内用又は社外用）を鍵保管部４０６から選択し、これを署名作成部４１８に渡す。署名作成部４１８は、その署名鍵を用いて処理内容要素３１０に対応する電子署名の値を求め、これら電子署名を示す署名情報要素３２２，署名値要素３２４及び鍵情報要素３２６を指示書分割／統合部４０４に渡す。指示書分割／統合部４０４は、受け取ったそれら各要素３２２，３２４及び３２６を処理内容要素３１０と組み合わせることで、フロー指示書を再構成し、これをネットワークＩ／Ｆ４０２から宛先のサーバに送信する。

【００７８】

なお、署名変換制御部４１２で署名の付け替えが不要と判定された場合（例えば社内から社内への指示書の場合）は、その旨が指示書分割／統合部４０４に伝

えられ、この判定結果を受けた指示書分割／統合部４０４は、ネットワークＩ／Ｆ部４０２から受信したフロー指示書３０をそのまま宛先のサーバへと送信する。

【００７９】

また、以上の例では、社内のサーバ２０は、社内ＣＡから受けた公開鍵証明書に対応する署名鍵しか用いなかったが、社内のサーバ２０が社外のＣＡからの公開鍵証明書を受けている場合もあり得る。このような場合、署名プロキシ装置４０は、社内のサーバ２０から社外サーバ６０宛のフロー指示書の署名検証により、その指示書に付されている署名が社内用のものか社外用のものかを判定し、社内用の場合は上述の署名の付け替えを行い、社外用の場合はその署名の付け替え処理を省略する。

【００８０】

図６及び図７を用いて説明した変形例では、社内の各サーバ２０が、フロー指示書３０の宛先が社外か社内かを判定し、社外の場合はフロー指示書３０を署名プロキシ装置４０に送っていたが、社内サーバ２０側でそのような判定を行わない方式も可能である。この方式では、署名プロキシ装置４０が社内のＬＡＮ５０とインターネットとの境界にゲートウェイとして設けられ、社内ＬＡＮ５０上からインターネットへ出ようとするフロー指示書３０を監視する。そして、署名プロキシ装置４０は、監視により見つけたフロー指示書３０の電子署名を検証し、その署名が社内用の公開鍵証明書に対応する秘密鍵を用いたものである場合は、上述の署名付け替え処理を行った上で、インターネット上の宛先サーバへと送信する。また、署名プロキシ装置４０は、インターネットから社内ＬＡＮ５０に入ろうとするフロー指示書の監視も行い、そのフロー指示書が社外用の公開鍵証明書に対応する秘密鍵により署名されたものである場合は、上述の署名の付け替え処理を行う。このような仕組みでも、図６及び図７の変形例と同様の効果が得られる。

【００８１】

また、署名プロキシ装置４０をアプリケーションサーバ２０の１つとし、フロー指示書３０中に署名プロキシ装置４０の処理内容を記述し、署名プロキシ装置

４０がそれに従って上述の署名付け替え処理を実行するようにしてもよい。

【００８２】

また、以上の例では、次にフロー指示書を送信する宛先装置が社内か社外かをフロー指示書に記述された当該宛先装置のＵＲＬに基づき判定したが、この他にも、宛先装置のＩＰアドレスやＦＱＤＮ（Fully Qualified Domain Name），電子メールアドレスなどに基づきその判定を行ってもよい。宛先装置のＩＰアドレスやＦＱＤＮ（Fully Qualified Domain Name），電子メールアドレスなどは、フロー指示書中に明示的に示される場合もあれば、その指示書をパケット送信する際のパケットヘッダに記述される場合もあるが、いずれの場合も、サーバ２０やフロー制御装置２５は、その場合に応じて宛先情報を取得し、その情報から宛先が社内か社外かを判定すればよい。

【図面の簡単な説明】

【図１】　連携サービスを実現するシステム構成の一例を説明するための図である。

【図２】　図１のシステムにおけるアプリケーションサーバの構成を説明するための図である。

【図３】　電子署名が施されたフロー指示書の記述例を示す図である。

【図４】　連携サービスを実現するシステム構成の別の例を説明するための図である。

【図５】　変形例における指示入力装置の構成を説明するための図である。

【図６】　別の変形例のシステム構成を説明するための図である。

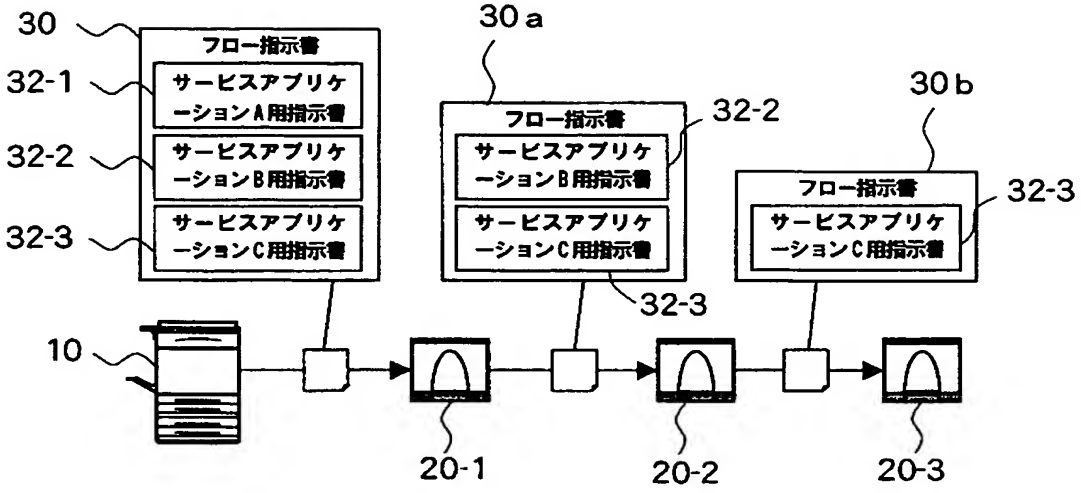
【図７】　図６の変形例における署名プロキシ装置の構成を説明するための図である。

【符号の説明】

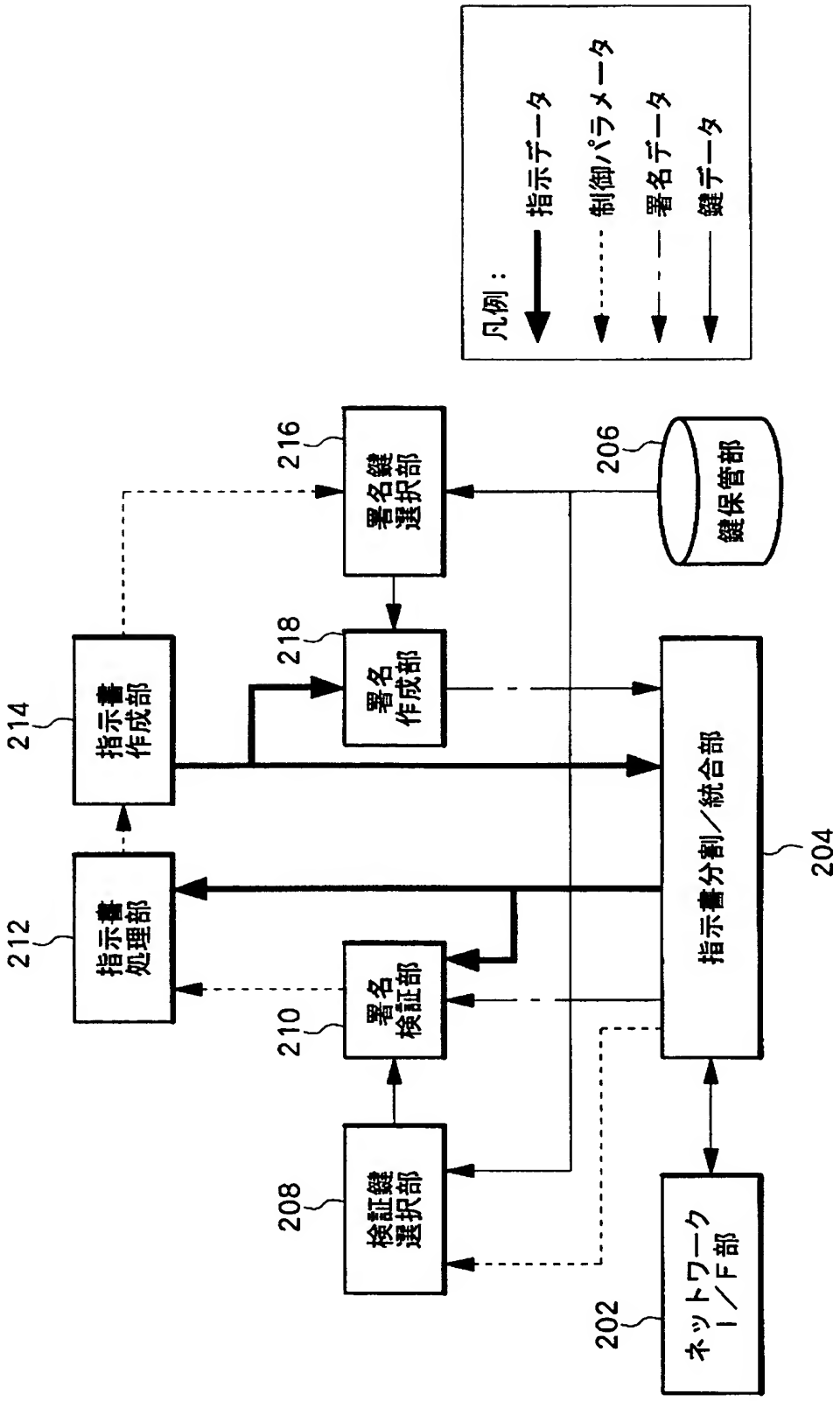
２０２　ネットワークＩ／Ｆ部、２０４　指示書分割／統合部、２０６　鍵保管部、２０８　検証鍵選択部、２１０　署名検証部、２１２　指示書処理部、２１４　指示書作成部、２１６　署名鍵選択部、２１８　署名作成部。

【書類名】　図面

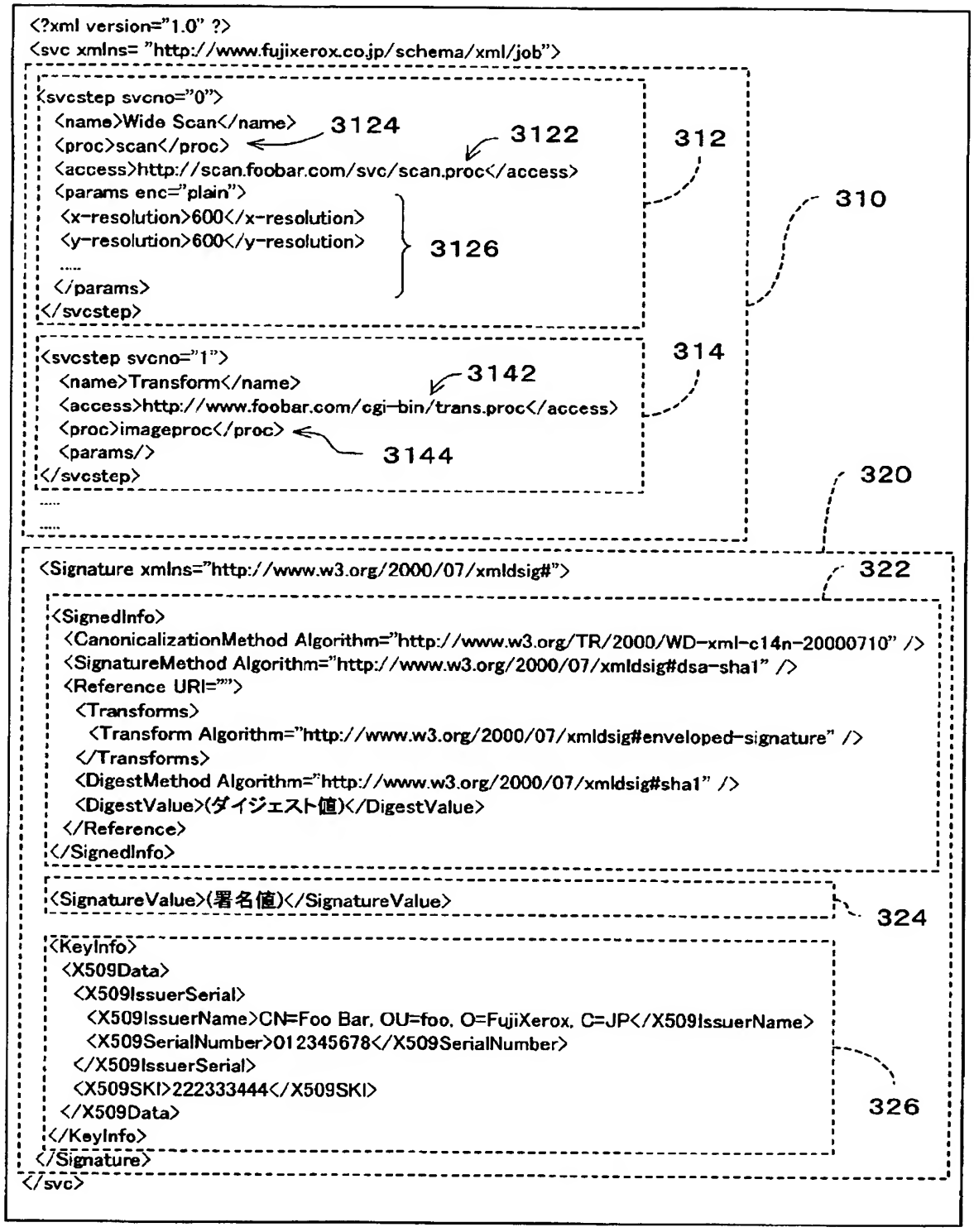
【図１】


30
フロー指示書
32-1
サービスアプリケーションA用指示書
32-2
サービスアプリケーションB用指示書
32-3
サービスアプリケーションC用指示書
30a
フロー指示書
32-2
サービスアプリケーションB用指示書
サービスアプリケーションC用指示書
32-3
30b
フロー指示書
32-3
サービスアプリケーションC用指示書
10
20-1
20-2
20-3

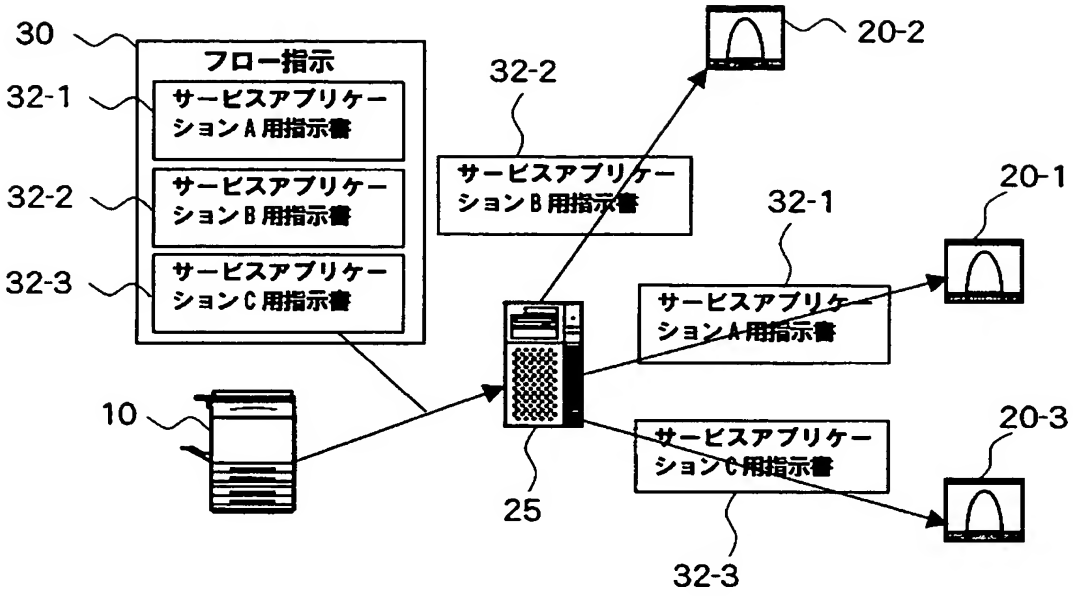
【図２】


凡例：
指示データ
制御パラメータ
署名データ
鍵データ
216
署名鍵選択部
206
鍵保管部
218
署名作成部
214
指示書作成部
204
指示書分割／統合部
212
指示書処理部
210
署名検証部
208
検証鍵選択部
202
ネットワークI／F部

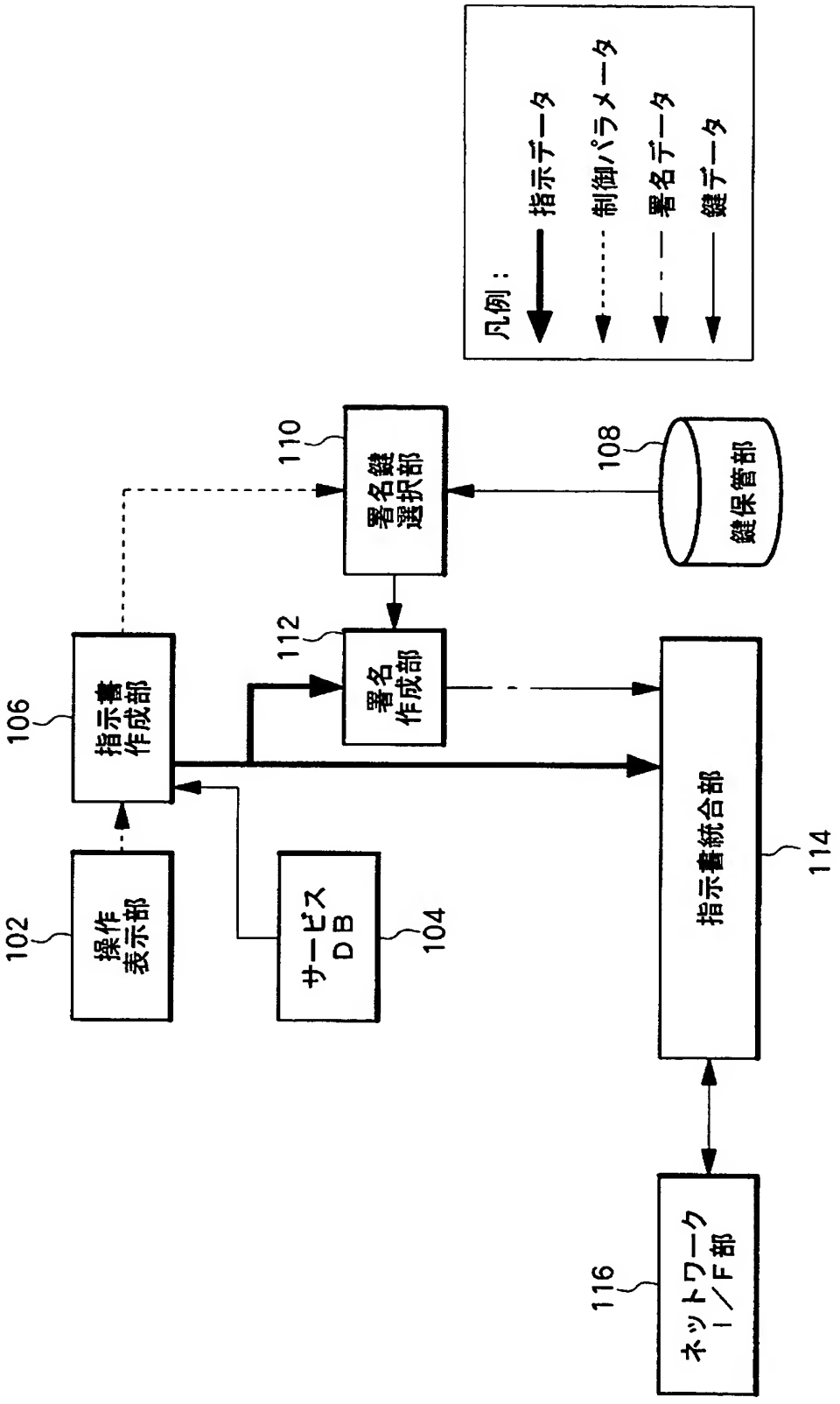
【図３】


<?xml version="1.0" ?>
<svc xmlns= "http://www.fujixerox.co.jp/schema/xml/job">
<svcstep svcno="0">
<name>Wide Scan</name>
<proc>scan</proc>
<access>http://scan.foobar.com/svc/scan.proc</access>
<params enc="plain">
<x-resolution>600</x-resolution>
<y-resolution>600</y-resolution>
.....
</params>
</svcstep>
3124
3122
3126
312
310
<svcstep svcno="1">
<name>Transform</name>
<access>http://www.foobar.com/cgi-bin/trans.proc</access>
<proc>imageproc</proc>
<params/>
</svcstep>
3142
3144
314
.....
.....
320
<Signature xmlns="http://www.w3.org/2000/07/xmldsig#">
322
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2000/WD-xml-c14n-20000710" />
<SignatureMethod Algorithm="http://www.w3.org/2000/07/xmldsig#dsa-sha1" />
<Reference URI="">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/07/xmldsig#enveloped-signature" />
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/07/xmldsig#sha1" />
<DigestValue>(ダイジェスト値)</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>(署名値)</SignatureValue>
324
<KeyInfo>
<X509Data>
<X509IssuerSerial>
<X509IssuerName>CN=Foo Bar, OU=foo, O=FujiXerox, C=JP</X509IssuerName>
<X509SerialNumber>012345678</X509SerialNumber>
</X509IssuerSerial>
<X509SKI>222333444</X509SKI>
</X509Data>
</KeyInfo>
326
</Signature>
</svc>

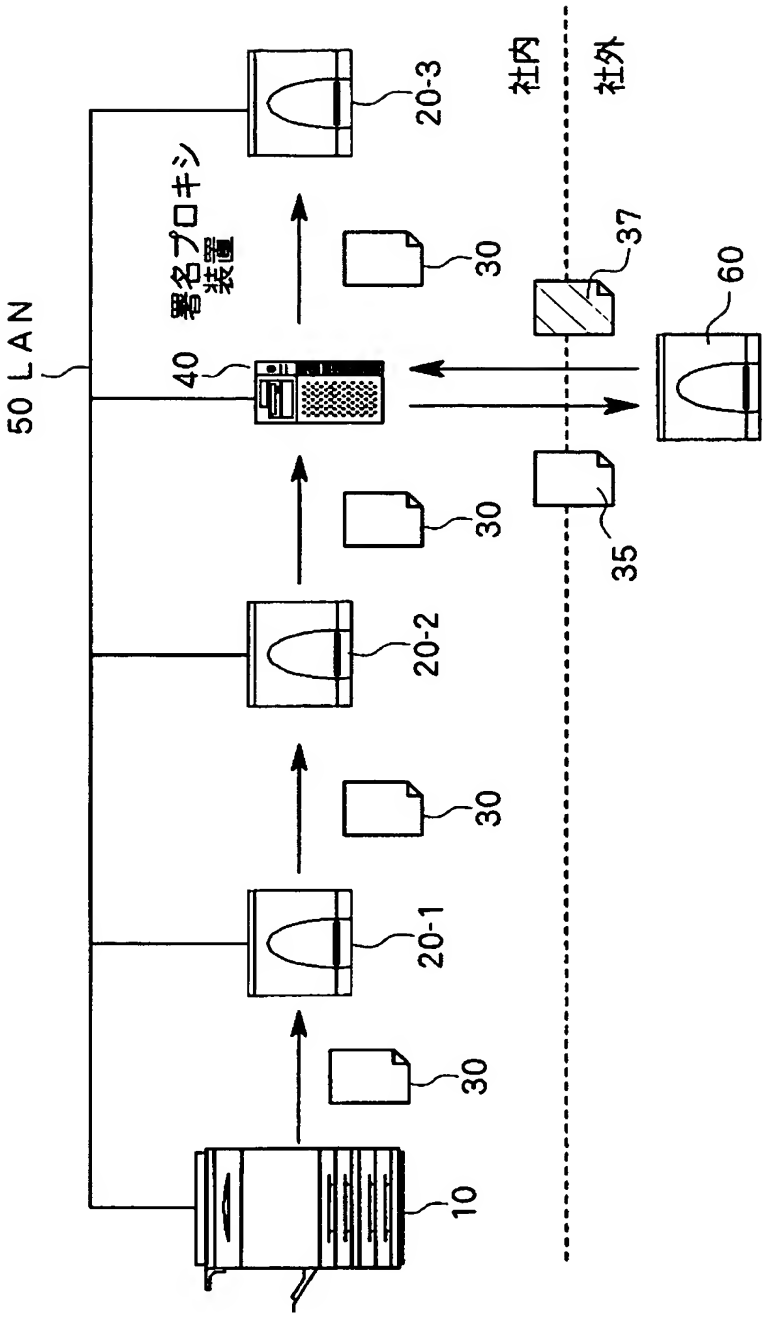
【図４】


30
フロー指示
32-1
サービスアプリケーションA用指示書
32-2
サービスアプリケーションB用指示書
32-3
サービスアプリケーションC用指示書
10
25
32-2
サービスアプリケーションB用指示書
20-2
32-1
サービスアプリケーションA用指示書
20-1
サービスアプリケーションC用指示書
20-3
32-3

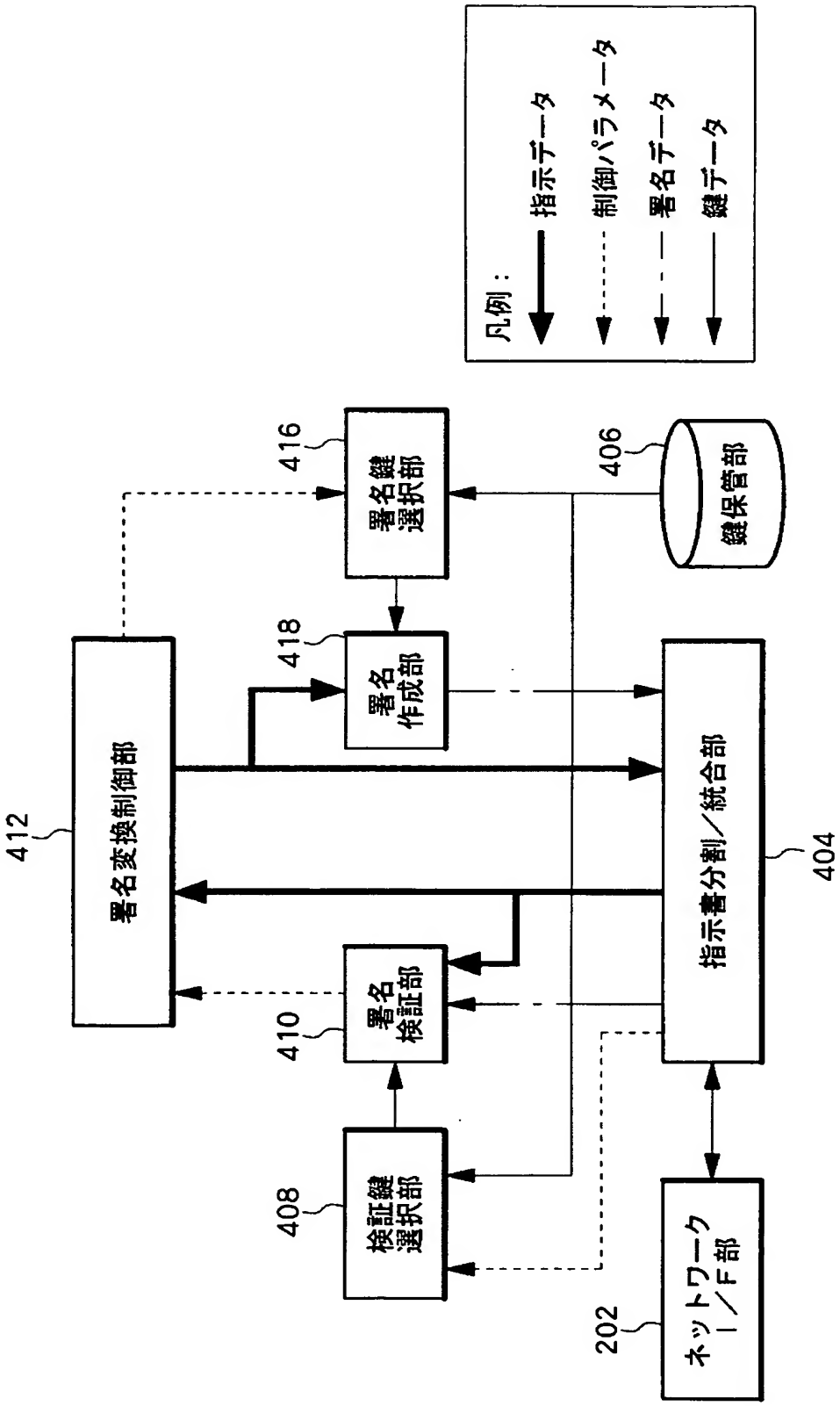
【図５】


凡例：
指示データ
制御パラメータ
署名データ
鍵データ
110
署名鍵選択部
108
鍵保管部
112
署名作成部
106
指示書作成部
102
操作表示部
サービスDB
104
指示書統合部
114
116
ネットワークI／F部

【図６】



【図７】


凡例：
指示データ
制御パラメータ
署名データ
鍵データ
署名鍵選択部
416
鍵保管部
406
署名作成部
418
署名変換制御部
412
指示書分割／統合部
404
署名検証部
410
検証鍵選択部
408
ネットワークI／F部
202

【書類名】　　要約書

【要約】

【課題】　社内サーバと社外サーバとの間の指示書のやりとりにおいて、電子署名の検証を容易にする。

【解決手段】　連携サービスの一部の処理を担う各サーバは、鍵保管部２０６に、それぞれ社内ＣＡと社外の公的ＣＡの各々から発行された公開鍵証明書に対応する秘密鍵を有している。署名鍵選択部２１６は、当該サーバの次に処理を実行するサーバが社内、社外のどちらの装置であるかを判別し、社内の場合は社内用の秘密鍵を、社外の場合は社外用の秘密鍵を選択する。署名作成部２１８は、その選択された秘密鍵を用いて、次のサーバへのフロー指示書のための電子署名の値を求める。指示書分割／統合部２０４は、フロー指示書に電子署名値を付加したものを、次のサーバに送信する。

【選択図】　　図２

特願２００３－０８２６１２

出　願　人　履　歴　情　報

識別番号　　［０００００５４９６］

１．変更年月日　　１９９６年　５月２９日
［変更理由］　　住所変更
住　所　　東京都港区赤坂二丁目１７番２２号
氏　名　　富士ゼロックス株式会社